IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH)
OF TARGET ELECTRONIC)
DEVICES AND EMAIL ACCOUNTS) CASE NO. 14-0557TJS
) 14-0558TJS
)
)
)

AFFIDAVIT IN SUPPORT OF SEARCH AND SEIZURE WARRANT

I, Kate N. Reilly, being first duly sworn state the following:

INTRODUCTION

1. I am a Special Agent of the United States Immigration and Customs Enforcement, Homeland Security Investigations (HSI), presently assigned to the Human Trafficking Unit located at the Custom House, Baltimore, Maryland. I have been employed with HSI since March 2009. Your affiant is currently assigned to the Human Smuggling and Trafficking unit. As part of my daily duties as an HSI agent, I investigate criminal violations relating to human trafficking including sex and labor trafficking in violation of 18 U.S.C. §§ 1589, 1590 and 1591 as well as interstate transportation for prostitution (Mann Act) in violation of 18 U.S.C. § 2421. I have received training in the area of human trafficking and have also participated in the execution of search warrants which involved sex trafficking and sex trafficking of minors. I have received formal training from HSI and other agencies in the area of internet crimes and investigation including the use of social networking sites and other internet facilities to coerce and/or facilitate prostitution of minors and adults in violation of 18 U.S.C. § 1591 and interstate prostitution (Mann Act) 18 U.S.C. § 2421.

JSH

2. I respectfully submit that probable cause exists to believe that the electronic devices described in Attachment A contain evidence, and are themselves instrumentalities, of criminal conduct committed by Michael BOSWELL, Catrina BATTLE, and others.

3. This affidavit is submitted in support of a search and seizure warrants for email accounts and electronic devices. I believe there is probable cause to believe that Michael BOSWELL has committed violations of 18 U.S.C. § 2422, coercion and enticement of an individual to travel in interstate commerce to engage in prostitution; and 18 U.S.C. § 2421, transportation of any individual interstate with the intent that the individual engage in prostitution or any sexual activity for which the individual can be charged with a criminal offense; and conspiracy to commit the above offenses in violation of 18 U.S.C. § 371. I further believe that there is probable cause to believe that a search of the email accounts and devices listed below will uncover evidence, fruits, and/or instrumentalities of these violations.

4. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of the aforementioned federal statutes are located within the email accounts described above. The information contained in this affidavit came from my own participation in the investigation described herein as well as other agents and officers involved in this investigation. I have not included each and every fact known to me or collectively known by agents and officers involved in this investigation, rather facts sufficient to establish probable cause.

JSH

5. This affidavit is submitted to search the email accounts listed below in paragraph 7, and the electronic devices listed in paragraphs 11 and 12.

EMAIL ACCOUNTS TO BE SEARCHED

6. The email accounts to be searched are: **fbm.entertainment2@gmail.com, fbm.entertainment3@gmail.com, fbm.entertainment4@gmail.com,** and **fbm.entertainment5@gmail.com**, maintained by Google, Inc. (Google), located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

7. This warrant application is governed by 18 U.S.C. § 2703(a), which permits governmental entities to require disclosure of the contents of stored electronic communications pursuant to a search warrant. Section 2703(a) further provides that such a warrant may be issued "by a court with jurisdiction over the offense under investigation." Moreover, §§ 2703(c)(1)(A) and (c)(2), provide that, in addition to the contents of electronic communications, the government may obtain by means of a search warrant any remaining types of records and information, such as computer logs and subscriber information, pertaining to a subscriber of an electronic communication service or remote computing service. Section 2703(c)(3) provides further that under such circumstances, no notice to the subscriber or customer is required.

8. This Court has jurisdiction to issue the requested search warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). The procedure by which the government will search the email accounts and seize the information contained is described in Attachments A1 and B2 hereto and below.

JSH

DEVICES TO BE SEARCHED

9. The target electronic devices to be examined are described herein and further described in Attachment A. The devices were seized on May 3, 2012 and January 3, 2013, by the Henrico County Police Department in Virginia.

10. The devices recovered on May 3, 2012 are:

a. One ZTE Cricket X500 cell phone;
b. One HP Model DV6-3134NR laptop, SN: CNF0428CJQ;
c. One Seagate 320 GB external hard drive, SN: 2GE1EFYW;
d. One Acer Model A500 tablet;
e. One Samsung Galaxy SII Model SPH-D710 cell phone with micro SD card adaptor;
f. One HTC PG86100 cell phone, SN: HT16MHX25064; and
g. One HTC PC36100 cell phone, SN: HT181HL07591.

11. The devices recovered on January 3, 2013 are:

a. One Samsung Galaxy Note II, SN: 99000210814214;
b. One Sprint HTC cell phone, SN: HT279S403073;
c. One Samsung cell phone, SN: 268435460803121059;
d. One Samsung cell phone, SN: R21c50chpsv;
e. One HTC PG76200 cell phone, SN: ht21bx002495;
f. One Blackberry cell phone, MEID: A000001c97f58f;
g. One Crystal View laptop, SKU: 887163; and
h. One Dell Inspiron laptop, SN: 18186943717.

12. The Devices are currently in storage at 40 S. Gay Street, Baltimore, Maryland. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of HSI.

13. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

JSIT

14. This is the third federal search warrant sought as part of this federal investigation into prostitution-related offenses by BOSWELL. BOSWELL was charged in a criminal complaint on October 22, 2013, with violations of 18 U.S.C. §§ 371, 2421, 2422. SAG-13-2501. That same day, United States Magistrate Judge Stephanie A. Gallagher authorized a search warrant for email accounts connected with this investigation. SAG-13-2502 & 2503. *See* Exhibit 1. In an Indictment returned by the Grand Jury for the District of Maryland on October 31, 2013, BOSWELL was charged with violations of 18 U.S.C. §§ 2421 & 2422. A second search warrant for electronic devices seized in Anne Arundel County on June 20, 2013, was authorized on December 18, 2013, by United States Magistrate Judge Stephanie A. Gallagher. *See* Exhibit 2. Trial is scheduled for April 14, 2013.

15. The two prior search warrants are attached as Exhibit 1 and Exhibit 2, and incorporated herein. Based on training and experience, as well as the investigation reflected in this affidavit, Exhibit 1, and Exhibit 2, I know that BOSWELL and co-conspirators have used email accounts in furtherance of criminal activities. Email accounts identified below in this affidavit have been linked to phone numbers, financial accounts, accounts on Backpage.com, and even listed as a "contact" email for persons wishing to pay for commercial sex acts.

16. I also know, based on training and experience, as well as the investigation reflected in this affidavit, Exhibit 1, and Exhibit 2, that BOSWELL and co-conspirators have made extensive use of electronic devices in carrying out their crimes. Phones in particular, have been used to communicate between BOSWELL, co-conspirators, prostitutes, and individuals seeking to pay for commercial sex acts. Electronic devices

JSH

have also been used to access email accounts, financial accounts, and accounts on Backpage.com. Forensics from electronic devices recovered on June 20, 2013, have also revealed photographs and other files used in Backpage.com advertisements for commercial sex acts.

A. Email Accounts

17. As set forth in Exhibit 2, a Samsung Galaxy Note 2 smartphone was seized from BOWELL in Anne Arundel County, Maryland, on June 20, 2013. It was seized at the same time BOSWELL was arrested as part of a prostitution sting. *See* Exhibit 2. Forensic analysis of BOSWELL's Samsung Galaxy Note 2 smartphone has since revealed that several email accounts were linked to this phone, including: fbm.entertainment@gmail.com,fbm.entertainment1@gmail.com, **fbm.entertainment2@gmail.com**, **fbm.entertainment3@gmail.com**, **fbm.entertainment4@gmail.com**, and **fbm.entertainment5@gmail.com**. The forensic analysis also showed an Internet history with numerous visits to the Backpage.com escort section including a link to edit/remove/re-post an ad linked to e-mail address fbm.entertainment1@gmail.com.[1] Forensic analysis of Boswell's phone also revealed text messages, pictures, and other files relating to prostitution and commercial sex acts.

18. A subpoena to Google revealed that five of these email accounts – fbm.entertainment1@gmail.com, **fbm.entertainment2@gmail.com**, **fbm.entertainment3@gmail.com**, **fbm.entertainment4@gmail.com**, **fbm.entertainment5@gmail.com** – were linked to the same secondary email account:

[1] fbm.entertainment@gmail.com and fbm.entertainment1@gmail.com, were the subject of the email search warrants sought pursuant to the affidavit at Exhibit 1.

JSH

m2ezze@yahoo.com. A subscriber is asked to provide a secondary email account by Google so there is an alternate means of contacting the subscriber for purposes such as password recovery or security notifications. That email account, m2ezze@yahoo.com, was the subject of a search warrant issued pursuant to the affidavit attached as Exhibit 1, based on a showing that email account was also linked to this offense. *See* Exhibit 1, ¶¶ 13-15.

19. I believe these email accounts contain fruits, instrumentalities of the federal crimes described above. The email accounts share a common name – "fbm.entertainment" – that has been linked to BOSWELL and this investigation. All the email accounts were linked to the phone seized from BOSWELL at the time of his arrest, such that he could send and receive messages from these accounts from his phone. And all of these emails have been linked to the same secondary email address. Accordingly, I believe there is probable cause to believe that they all contain fruits, instrumentalities, and evidence of this offense.

B. Henrico County Evidence

20. On May 3, 2012 the Henrico County Police Department's (HCPD) Vice Unit conducted a prostitution sting in response to a Backpage.com advertisement for commercial sex acts. An undercover detective responded to the advertisement and was directed to a room at the Clarion Inn Hotel. Detectives set up surveillance at the hotel.

21. As the undercover detective approached the hotel, other officers saw two individuals (later identified as BOSWELL and BATTLE) in a white Ford Expedition drive slowly out of the parking lot. Detectives observed that Boswell appeared to be

watching them in a manner consistent with counter-surveillance, and decided to follow the Ford Expedition. The followed the SUV to a local Walmart, where BOSWELL dropped off BATTLE and then proceeded to park the SUV. A detective then approached BOSWELL as he was getting out of the SUV. After the detective identified himself, BOSWELL reached back into the car so the detective the detective detained BOSWELL for safety reasons. BOSWELL admitted to staying at the Clarion Hotel with WITNESS1 and BATTLE, but claimed to be a party planner and denied being involved in prostitution

22. WITNESS1 was arrested at the Clarion Inn Hotel following the sting. She was *Mirandized*, and consented to giving a statement to HCPD detectives.

a. WITNESS1 said she was contacted by a family friend named "Trina," who was later identified as BATTLE. BATTLE told WITNESS1 that she was in Richmond, VA, and asked WITNESS1 to join her because she can help her make money. WITNESS1 admitted that she knows BATTLE is a prostitute and accepts money for sex and that BOSWELL is a pimp. WITNESS1 said she agreed to travel from Raleigh, NC to Richmond, VA, and BATTLE booked and paid for her bus ticket online. Detectives seized a Greyhound bus ticket from May 1, 2012, that appears to corroborate this.

b. When she arrived at the Clarion Inn Hotel there was a man there named "Mike," later identified as BOSWELL. WITNESS1 stated that BOSWELL posted an advertisement on Backpage.com, advertising commercial sex acts, on the night she arrived in Richmond – approximately May 1, 2012. She also admitted to detectives that she had seen four clients prior to her date with the undercover officer and for at least three of these dates she gave a portion of her proceeds to BOSWELL.

JSH

23. As a result of this prostitution sting, HCPD detectives seized four cell phones, one laptop, one external hard drive and one tablet from the hotel room, and from the persons of BOSWELL, BATTLE and WITNESS1: a **ZTE Cricket X500 cell phone**; **HP Model DV6-3134NR laptop, SN: CNF0428CJQ**; **Seagate 320 GB external hard drive, SN: 2GE1EFYW**; **Acer Model A500 tablet**; **Samsung Galaxy SII Model SPH-D710 cell phone with micro SD card adaptor**; **HTC PG86100 cell phone, SN: HT16MHX25064**; and **HTC PC36100 cell phone, SN: HT181HL07591**.

24. On January 3, 2013, HCPD initiated another prostitution investigation stemming from an advertisement for commercial sex acts on Backpage.com. HCPD responded to the advertisement, and were told that the prostitute was located in room 138 at the Red Roof Inn on 5209 Williamsburg Road in Richmond. Based on this information, HCPD detectives started surveillance at the Red Roof Inn.

25. Surveillance reports state that BOSWELL, WITNESS2, and a female later identified as WITNESS3, entered a dark colored sedan and drove to a residence in Hopewell, VA. WITNESS2 was seen exiting the car and entering the residence. The surveillance team then followed BOSWELL and WITNESS3 as they drove to an address in Richmond, where WITNESS3 was seen exiting the vehicle and entering a residence. On both occasions, HCPD interviewed the clients or "johns" after WITNESS2 and WITNESS3 left their respective "dates." Both "johns" admitted to engaging in commercial sex with the women BOSWELL was with. BOSWELL, WITNESS2 and WITNESS3 eventually returned to the Red Roof Inn.

26. BOSWELL, WITNESS2, and WITNESS3 were arrested. At the time of this arrest, HCPD detectives seized phones and computers from the hotel room at the Red

Roof Inn, and the persons of BOSWELL, WITNESS2 and WITNESS3: **Samsung Galaxy Note II, SN: 99000210814214; Sprint HTC cell phone, SN: HT279S403073; Samsung cell phone, SN: 268435460803121059; Samsung cell phone, SN: R21c50chpsv; HTC PG76200 cell phone, SN: ht21bx002495; Blackberry cell phone, MEID: A000001c97f58f; Crystal View laptop, SKU: 887163**; and **Dell Inspiron laptop, SN: 18186943717**.

27. Both WITNESS2 AND WITNESS3 subsequently consented to voluntary interviews.

a. WITNESS2 told detectives she had been a prostitute since she was seventeen. She stated that she had been prostituting for BOSWELL for some time, and that she, WITNESS3, and BATTLE traveled to Hopewell, VA for WITNESS3's "date" i.e. a commercial sex act. WITNESS2 said she received $160 for one hour of sexual intercourse. She held this money until she returned to the hotel, at which point she gave it to all BOSWELL for "safekeeping." She indicated that she had traveled with BOSWELL from North Carolina to Virginia for the purpose of prostitution. She also stated that she had traveled to Pittsburgh, PA with BOSWELL for prostitution and that he had paid for her bus ticket from North Carolina to Pennsylvania. It is noted that a subpoena response from Backpage.com confirms that on December 16, 2012, an advertisement for escort services was posted in Pittsburgh, PA. This Backpage.com account used to post that advertisement had a subscriber email address of m2ezze@yahoo.com, which – as described above – is known to be used by BOSWELL.

b. WITNESS3 stated that she had been prostituting for BOSWELL since Summer 2012. She stated that she gave the money from prostituting herself to

JSH

BOSWELL. She had traveled with BOSWELL for the purpose of prostitution to several states, including Pennsylvania, Virginia, New Jersey, and North Carolina.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on the electronic devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

JSH

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data, with internal storage on a number of electronic devices containing slightly less. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

f. Thus, the ability to retrieve residue of an electronic file from a hard drive or internal storage of other types of electronic devices depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above described information will be recovered during forensic analysis.

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct

JSH

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

JSH

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

BACKGROUND CONCERNING EMAIL

31. In my training and experience, I have learned that companies such as Google provide a variety of online services, including electronic mail ("email") access, to the public. That allows subscribers to obtain email accounts like the email accounts listed in Attachment A. Subscribers obtain an account by registering with the company. During the registration process, the company asks subscribers to provide basic personal information. Therefore, the computers of the company are likely to contain stored electronic communications (including retrieved and unretrieved email for subscribers) and information concerning subscribers and their use of email services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

32. An email account subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the company. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

33. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account.

JSH

Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

34. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

35. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training

and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

CONCLUSION

36. Based on your affiant's training and experience, your Affiant respectfully submits that probable cause exists to search the Devices listed in Attachment A; and the email accounts listed in Attachment A1. Therefore, I respectfully request that the attached warrants be issued.

I declare under penalty of perjury that the foregoing is true and correct.

Kate N. Reilly
Special Agent, Homeland Security Investigations

Sworn and subscribed to before me on this 6th day of March, 2014.

Timothy J. Sullivan
United States Magistrate Judge

JSA

14-0557TJS 14-0558TJS

ATTACHMENT A
(Devices to be Searched)

a. One ZTE Cricket X500 cell phone;
b. One HP Model DV6-3134NR laptop, SN: CNF0428CJQ;
c. One Seagate 320 GB external hard drive, SN: 2GE1EFYW;
d. One Acer Model A500 tablet;
e. One Samsung Galaxy SII Model SPH-D710 cell phone with micro SD card adaptor;
f. One HTC PG86100 cell phone, SN: HT16MHX25064;
g. One HTC PC36100 cell phone, SN: HT181HL07591;
h. One Samsung Galaxy Note II, SN: 990002108142l4;
i. One Sprint HTC cell phone, SN: HT279S403073;
j. One Samsung cell phone, SN: 268435460803121059;
k. One Samsung cell phone, SN: R21c50chpsv;
l. One HTC PG76200 cell phone, SN: ht21bx002495;
m. One Blackberry cell phone, MEID: A000001c97f58f;
n. One Crystal View laptop, SKU: 887163; and
o. One Dell Inspiron laptop, SN: 18186943717.

JSA

14-0557TJS 14-0558TJS

ATTACHMENT B

1. All information and records on the devices described in Attachment A that relate to violations of 18 U.S.C. §§ 2421, 2422 and 371 and involve BOSWELL and possible co-conspirators, including:

a. the communications and records of communications between BOSWELL, and possible co-conspirators;

b. any information regarding prostitution and/or escort services, including information about individuals involved in prostitution and/or escort services, and any information regarding recruitment, enticement or travel for the purpose of prostitution and/or escort services;

c. any information regarding the advertising of prostitution and/or escort services, including all records and communications relating to Backpage.com, fbm1entertainment.escort-site.com, F.B.M. Party Planners (FBM), Mobile Mixtape Entertainment, and any other business or websites used to advertise prostitution and/or escort services;

d. any information showing association between BOSWELL, WITNESS1, WITNESS2, and any others involved in prostitution and/or escort services;

e. all bank records, checks, credit card bills, account information, and other financial records;

f. any and all evidence of passwords needed to access any of the subject devices;

g. any and all records, showing dominion, ownership, custody, or control over the any of the subject devices;

h. All records and communications related to travel and location, including reservations or payments for hotel rooms and transportation such as payments for gas, rental cars, Greyhound bus, Amtrak, airlines, or other modes of transportation.

2. Evidence of user attribution showing who used or owned the phones at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Any of the items described in paragraphs 1 through 3 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form. The search procedure of the electronic data contained in computer operating software or memory devices shall include the following techniques which shall be used to minimize the risk that those conducting the search will view information not within the scope of the warrant:

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

4. If after performing these procedures, the directories, files or storage areas do not reveal evidence of violations of 18 U.S.C. §§ 2421, 2422 and 371, the further search of that particular directory, file or storage area, shall cease.

JSH

14-0557TJS 14-0558TJS

ATTACHMENT A1
(Google)

ITEMS TO BE SEIZED AND SEARCHED

This warrant applies to information associated with the e-mail accounts

fbm.entertainment2@gmail.com
fbm.entertainment3@gmail.com
fbm.entertainment4@gmail.com
fbm.entertainment5@gmail.com

which are stored at premises owned, maintained, controlled, or operated by Google Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

JrH

14-0557TJS 14-0558TJS

ATTACHMENT B1
(Google)

I. Information to be disclosed by the Provider.

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A, for the period from June 1, 2010, to October 21, 2013:

1. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

The types of service utilized;

3. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

4. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 371, 2421 & 2242, involving email accounts listed in Attachment A; including, but not limited to:

a. All records and communications relating to Backpage.com, fbm1entertainment.escort-site.com, F.B.M. Party Planners (FBM), Mobile Mixtape Entertainment, and any other business or website websites used to advertise prostitution and/or escort services;

b. All records and communications related to travel, including reservations or payments for hotel rooms and transportation such as payments for gas, rental cars, Greyhound bus, Amtrak, airlines, or other modes of transportation.

c. All records and communications related to use of credit cards, including prepaid credit cards;

d. All records and communications concerning prostitution and all communications with any individuals engaged in or recruited for prostitution;

e. All records, communications, images, or videos depicting individuals who are involved in prostitution or who are being recruited into prostitution;

f. All records and images of identity documents;

g. All records showing association between anyone involved in prostitution or violations of 18 U.S.C. §§ 371, 2421, and 2242, including Michael Boswell

and Catrina Battle.

2. Records relating to who created, used, or communicated with e-mail accounts email accounts listed in Attachment A, including, but not limited to, account holder's name, address, phone number, and alternate email address; account creation data including account creation date; IP log data for account; contacts; emails showing user attribution for account.

14-0557TJS 14-0558TJS

EXHIBIT 1

JSH

FILED ENTERED
LODGED RECEIVED

OCT 22 2013

AT BALTIMORE
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY DEPUTY

THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND

BALTIMORE DIVISION

IN THE MATTER OF A CRIMINAL COMPLAINT for MICHAEL DARNELL BOSWELL, and SEARCH WARRANTS FOR	13-2501SAG
GMAIL ACCOUNTS	Case No. 13-2502SAG
fbm.entertainment@gmail.com fbm.entertainment1@gmail.com	
YAHOO! ACCOUNTS	13-2503SAG
michellebella96@yahoo.com m2ezze@yahoo.com	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT AND CRIMINAL COMPLAINT

I, Kate Reilly, being duly sworn, depose and states as follows:

1. I am a Special Agent of the United States Immigration and Customs Enforcement, Homeland Security Investigations (HSI), presently assigned to the Human Trafficking Group located at the Custom House, Baltimore, Maryland. I have been employed with HSI since March 2009. As part of my daily duties as an HSI agent, I investigate criminal violations relating to human trafficking including sex and labor trafficking in violation of 18 U.S.C. §§ 1589, 1590 and 1591 as well as interstate prostitution (Mann Act) in violation of 18 U.S.C. §§ 2421, 2422. I have received training in the area of human trafficking and have also participated in the execution of search warrants which involved sex trafficking and sex trafficking of minors. I have received formal training from HSI and other agencies in the area of internet crimes and

investigation including the use of social networking sites and other internet facilities to coerce and/or facilitate prostitution of minors and adults in violation of 18 U.S.C. § 1591 and interstate prostitution (Mann Act) 18 U.S.C. § 2421. As a federal agent, your Affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to affect arrests and execute warrants issued under the authority of the United States.

2. This affidavit is submitted in support of a criminal complaint for Michael Darnell BOSWELL and for search and seizure warrants for email accounts. I believe there is probable cause to believe that Michael BOSWELL has committed violations of 18 U.S.C. § 2422, coercion and enticement of an individual to travel in interstate commerce to engage in prostitution; and 18 U.S.C. § 2421, transportation of any individual interstate with the intent that the individual engage in prostitution or any sexual activity for which the individual can be charged with a criminal offense; and conspiracy to commit the above offenses in violation of 18 U.S.C. § 371. I further believe that there is probable cause to believe that a search of the email accounts listed below will uncover evidence, fruits, and/or instrumentalities of these violations.

3. The email accounts to be searched are

a. **fbm.entertainment@gmail.com** and **fbm.entertainment1@gmail.com,** maintained by Google, Inc. (Google), located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

b. **michellebella96@yahoo.com,** and **m2ezze@yahoo.com,** maintained by Yahoo! headquartered at 701 First Avenue, Sunnyvale, CA 94089.

4. This Court has jurisdiction to issue the requested search warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a),

(b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). The procedure by which the government will search the email accounts and seize the information contained is described in Attachments A and B hereto and below.

5. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of the aforementioned federal statutes are located within the email accounts described above. The information contained in this affidavit came from my own participation in the investigation described herein as well as other agents and officers involved in this investigation. I have not included each and every fact known to me or collectively known by agents and officers involved in this investigation, rather facts sufficient to establish probable cause.

BACKGROUND OF THE INVESTIGATION

6. On June 19, 2013, Anne Arundel County Police Department's (AAPD) Vice Unit initiated an investigation into suspected prostitution activity at the Microtel Hotel (Microtel) located at 1170 Winterson Road, Linthicum, MD 21090. On this date, AAPD detectives accessed the "Escort" section of the website Backpage.com and located an advertisement that depicted photos of a black-female in partially nude and provocative poses.[1] The advertisement displayed the phone number ***-***-2668 and instructed the potential customer to call or text this number to set up a "date." Investigators, based on their training experience, determined the advertisement was consistent with an offer for commercial sexual services.

7. Later on June 19, 2013, an AAPD detective, acting in an undercover capacity, sent a text to this same number stating that he just got off work, was looking for an hour long

[1] Backpage.com is an online classified site that is commonly used to advertise for prostitution and sexual services.

appointment, and wanted to know how much an hour appointment would cost. The detective received a text message in reply, asking if the undercover detective wanted to visit her at her location or meet at his location. The undercover detective replied that he wanted to meet at her location. The response to this stated that it would be $150 for an hour long appointment. The undercover detective also inquired about "backyard play," or anal sex, which increased the rate to $200. Upon agreeing to this amount, the undercover detective was then directed to the Microtel and more specifically, room 240. The undercover detective later canceled the "date;" but AAPD detectives maintained surveillance at the Microtel.

8. During that surveillance, AAPD detectives observed a black male, later identified as Michael Darnell BOSWELL (DOB **/**/1983), driving a white Ford Expedition with North Carolina registration "ZTE 3073." Detectives watched BOSWELL drive from the Microtel to a nearby Wendy's restaurant and 7-11. Upon his return to the Microtel, detectives observed BOSWELL enter room 240 with a Wendy's bag and then exit the room without it. Hotel records indicate that room 240 and also room 242 were registered to a female, later identified to law enforcement and referred to herein as "A.G.," with an arrival date of June 18, 2013 and a departure date of June 19, 2013 that was later extended to June 20, 2013, and both rooms were paid for in cash.

9. Detectives later surveilled BOSWELL driving the Ford Expedition to a nearby Walmart. Detectives observed A.G. and R.T. exit BOSWELL's vehicle and enter the Walmart. A.G. and R.T. later returned to the vehicle and were then driven by BOSWELL to the Microtel. Upon their return, AAPD detectives observed A.G. and R.T. enter room 240. BOSWELL remained in his vehicle at this time.

10. On June 20, 2013, AAPD detectives returned to the Microtel and observed the white Ford Expedition in the parking lot. At approximately 10:28 am, a different detective, acting in an undercover capacity, texted the phone number in the same Backpage ad from the previous day (***-***-2668). A text conversation was initiated and an outcall "date"[2] was set up between the undercover detective and the female in the Backpage ad at the Red Roof Inn located at 827 Elkridge Landing Road, Linthicum, MD.

11. After the "date" for commercial sex was set up, surveillance teams observed BOSWELL drive A.G. in the Ford Expedition from the Microtel to the Red Roof Inn. The undercover detective directed A.G. to room 236 at the Red Roof Inn. Once A.G. entered the hotel room, the undercover detective asked her if she had a condom to which she replied "yes" and removed one from the small, black bag she was carrying. A.G. was arrested by AAPD and charged with prostitution and related offenses. BOSWELL was also arrested at a nearby parking lot, and R.T. was arrested at the Microtel in room 242. A search warrant was executed for rooms 240 and 242 at the Microtel and the Ford Expedition.

12. In a voluntary interview, A.G. provided information to law enforcement. She stated that BOSWELL recruited her at a party in North Carolina, and arranged for her to travel from Greensboro, NC, to Richmond, VA, via a Greyhound Bus that was purchased for her. This was corroborated by a Greyhound Bus ticket, in A.G.'s name, for such a trip recovered during the search of the Microtel. Once in Richmond, A.G. met up with BOSWELL and R.T., and, at BOSWELL's direction, began working as a prostitute in Virginia. She also stated that BOSWELL transported her and R.T. to Maryland for the purpose of further engaging in

[2] Based on my training and experience, I know that an "outcall" is a an appointment for commercial sex where the prostitute travels to the customer's location.

prostitution. She stated that BOSWELL would communicate directly with the sex customers, and then inform her when she had a "date" set up. Investigators

13. Pursuant to a subpoena to Backpage.com discussed above, Backpage provided records that showed, *inter alia*, that the customer account associated with the Backpage advertisement above had as its associated email address **fbm.entertainment1@gmail.com**. FBM Entertainment is a business owned by BOSWELL, as described below, Para. 16. Backpage requires account holders to provide an email address, which Backpage uses for all customer communications, such as confirmation of the posting of an advertisement, receipts for payments, and general account information. The subpoena response shows multiple advertisements for "escort services" consistent with advertisements for commercial sex (i.e. prostitution) were posted on Backpage.com with this same account from at least April 2013 through July 2013. These advertisements advertised services in various states including North Carolina, Virginia, Washington, DC and Maryland.

a. The subpoena response showed the account associated with **fbm.entertainment1@gmail.com** was used to post advertisements for commercial sexual services in Richmond, Northern Virginia and Maryland. For instance, on June 12, 2013, an advertisement for sexual services in Richmond, Virginia from "Ms. Monroe" was posted, showing pictures of R.T. A similar advertisement for sexual services in Richmond, Virginia from "Kimberly" (A.G.) was also posted. Similar advertisements were posted against on June 13, 2013.

b. On June 14, 2013, an advertisement for sexual services in Springfield/Northern Virginia from R.T was posted. A similar advertisement for R.T. was

reposed on the June 15, 16, and 17. A similar advertisement for sexual services in Springfield/Northern Virginia from A.G. was also posted on June 16 and 17.

c. On June 18, 2013, Backpage ads were posted advertising sexual services by R.T. and A.G. in the Baltimore/BWI area. The IP addresses used to make these posts was registered to the Microtel where BOSWELL, A.G and R.T. were staying at the time AAPD was conducting the undercover operation.

14. The Backpage subpoena also showed that most of the associated advertisemetns for commercial sex acts were paid for with American Express credit card ending with 9231. A subpoena to American Express showed that the American Express customer is Michael BOSWELL, DOB **/**/1983, 1500 Burgundy Street, Apt. A, Raleigh, NC 27610, phone number ***-***-9148, and that the email associated with the account was **m2ezze@yahoo.com**.

a. The American Express transaction records also show numerous payments made to BACKPAGE.COM and merchants in North Carolina, Virginia, and Maryland. In the weeks following BOSWELL's arrest in Anne Arundel County, several transfers of money were made from the American Express account to "catrina battle" via the email address **michellebella96@yahoo.com**. In my training and experience, online payment services (such as Paypal) commonly allow payments to be made to an account identified by an email address. The email address serves as the account identifier (much like an account number serves as the identifier for a traditional bank account). I therefore believe that the email address **michellebella96@yahoo.com** is an email address associated with an account used for transfer payments relating to the commercial sex acts targeted by this investigation.

b. Witnesses have advised investigators that Battle is BOSWELL's fiancée.

Also, at the time of his arrest, BOSWELL told detectives that Battle was his girlfriend and asked that she be notified of his arrest. Battle has prior charges for prostitution, including a recent arrest on July 24, 2013 in Raleigh, North Carolina resulting in charges for prostitution-related offenses. According to subpoena results from Backpage.com, some of the Backpage postings for commercial sex acts associated with this investigation list "Catrina Battle" as the name on the account making the posting.

15. In my training and experience, financial accounts (such as accounts with banks, credit cards, and payment providers) often have an email address associated with account. The financial institutions will typically send emails to those associated accounts containing information related to the account – including summary information about the account, information about specific transactions, and responses to questions from the customer. I therefore believe there is probable cause to believe that the email accounts **fbm.entertainment1@gmail.com**, **m2ezze@yahoo.com**, and **michellebella96@yahoo.com**, will contain records and information about transactions associated with violations of 18 U.S.C. §§ 2421 & 2422.

16. BOSWELL is a self-proclaimed "party planner" and owns a business called F.B.M. Party Planners (FBM) and Mobile Mixtape Entertainment. At the time of arrest, BOSWELL had in his wallet two business licenses for FBM and Mobile Mixtape. He also had an IRS Form 8832, Entity Classification Election, in his wallet, which contained the business name of Mobile Mixtape and an Employer Identification Number (EIN). These documents show both businesses are registered to the address 2010 Hodge Creek Drive, Apt. 104, Raleigh, NC 27609.

a. The website for FBM is fbm1entertainment.escort-site.com. An open-source review of this website confirmed that this website advertises escort services and prostitution. Under the "photos" section of the website there are multiple females, such as "Candy" and "Mz Slim," in partially nude photographs. The "services" section of the website indicates the types of services provided by FBM, such as "Fetish/Fantasy, Role Play, Mistress Worship." There is also a list on the site entitled "My Escort Services," which lists common terms used in prostitution and their definitions, such as "69 (69 sex), BJ (blow job), CBJ (Covered Blow Job; Oral sex with a condom)."

b. The search warrant executed by AAPD at the Microtel also recovered a notepad with the term "FBM 4 Lyfe" handwritten on it. Furthermore, in a voluntary interview with your affiant, R.T. stated that when she met BOSWELL at a party in North Carolina he gave her a business card with "FBM" on the front of it. BOSWELL told her that "FBM" stands for Future Black Millionaire.

c. The "contact" section of the website, fbm1entertainment.escort-site.com, states that customers and others can contact "FBM" at the email address **fbm.entertainment@gmail.com**. Based on my training and experience, I know that online businesses often provide a contact email address to answer customer questions, to sell and facilitate the sale of products and services (legitimate or illegitimate), and to handle financial transactions related to the online business. I therefore believe there is probable cause to believe that the contents of the email account **fbm.entertainment@gmail.com** will contain evidence, fruits, and/or instrumentalities of violations of 18 U.S.C. §§ 2421 & 2422.

17. BOSWELL was charged in in Anne Arundel County Circuit Court with various

offenses, including Human Trafficking, Prostitution, and Possession of Marijuana. He is presently detained pending trial on these charges.

18. Prior to his arrest in Maryland, BOSWELL had multiple arrests in New Jersey, North Carolina, and Virginia, including charges for prostitution and related offenses, as follows:

a. On November 24, 2010, BOSWELL was arrested and charged in Raleigh, North Carolina with 1) Possession of a Firearm by a Felon, 2) Possession of Marijuana Up to ½ Ounce, and 3) Aid and Abet Prostitution. On May 20, 2013, he was convicted of Possession of a Firearm by a Felon, which is a felony charged.

b. On April 20, 2011, BOSWELL was arrested and charged in Raleigh, North Carolina for Maintain Place for Prostitution, which was dismissed.

c. On May 3, 2012, BOSWELL was arrested in Henrico County, Virginia for 1) Two Counts of Prostitution: Receive Earnings (Pandering), 2) Possess Marijuana, 3) Prostitution: Aid, and 4) Prostitution: Keep/Reside in Bawdy Place. All charges were dismissed.

d. On January 4, 2013, BOSWELL was arrested in Henrico County, Virginia for 1) Prostitution: Use Vehicle to Aid, 2) Two Counts Prostitution: Aid, 3) Prostitution: Keep/Reside in Bawdy Place, 4) Weapon: Possess by Felon (Not Firearm), and 5) Possess Marijuana 2+ Offense. BOSWELL was found not guilty of Possess Marijuana 2+ Offense. There was no disposition for Weapon: Possess by Felon (Not Firearm) and all other charges were dismissed.

e. On March 11, 2013, BOSWELL was arrested and charged in Henrico County, Virginia for 1) Six counts of Prostitution: Receive Earnings (Pandering), 2) Prostitution: Aid, 3) Two counts of Prostitution: Use Vehicle to Aid, 4) Two counts of Prostitution: Cause

Person to Enter Bawdy Place, and 5) Prostitution: Keep/Reside In Bawdy Place. BOSWELL was released on bond for these charges and was awaiting trial at the time he was arrested in Maryland. At the time of his arrest in Maryland, he was also on probation at the time for a prior firearm offense.

BACKGROUND CONCERNING EMAIL

19. In my training and experience, I have learned that companies such as Yahoo and Google provide a variety of online services, including electronic mail ("email") access, to the public. That allows subscribers to obtain email accounts like the email accounts listed in Attachment A. Subscribers obtain an account by registering with the company. During the registration process, the company asks subscribers to provide basic personal information. Therefore, the computers of the company are likely to contain stored electronic communications (including retrieved and unretrieved email for subscribers) and information concerning subscribers and their use of email services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. An email account subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the company. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

21. In my training and experience, email providers generally ask their subscribers to

provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

23. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a

result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

24. This warrant application is governed by 18 U.S.C. § 2703(a), which permits governmental entities to require disclosure of the contents of stored electronic communications pursuant to a search warrant. Section 2703(a) further provides that such a warrant may be issued "by a court with jurisdiction over the offense under investigation." Moreover, §§ 2703(c)(1)(A) and (c)(2), provide that, in addition to the contents of electronic communications, the government may obtain by means of a search warrant any remaining types of records and information, such as computer logs and subscriber information, pertaining to a subscriber of an electronic communication service or remote computing service. Section 2703(c)(3) provides further that under such circumstances, no notice to the subscriber or customer is required.

CONCLUSION

25. Based upon the information outlined above, there is probable cause to believe that Michael BOSWELL has violated 18 U.S.C. § 2422(a), coercion and enticement of an individual to travel in interstate commerce to engage in prostitution; 18 U.S.C. § 2421, transportation of any individual interstate with the intent that the individual engage in prostitution or any sexual activity for which the individual can be charged with a criminal offense; and conspiracy to commit the above offenses in violation of 18 U.S.C. § 371.

26. Furthermore, I submit that there is probable cause to believe that evidence, fruits, and/or instrumentalities of these violations is currently located in the email accounts specified in

Attachment A. Therefore, I respectfully request that the attached warrant be issued authorizing the search of the email accounts listed in Attachment A and the seizure of the items listed in Attachment B.

Kate N. Reilly, Special Agent
Homeland Security Investigations (HSI)
Department of Homeland Security

Sworn and subscribed before me
this 22nd day of October, 2013

HONORABLE STEPHANIE A. GALLAGHER
UNITED STATES MAGISTRATE JUDGE

14-0557TJS 14-0558TJS
EXHIBIT 2

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF TARGET ELECTRONIC DEVICES LISTED IN ATTACHMENT A, CURRENTLY IN LAW ENFORCEMENT POSSESSION	)	CASE NO. 13-2995SAG

AFFIDAVIT IN SUPPORT OF SEARCH AND SEIZURE WARRANT

I, Kate N. Reilly, being first duly sworn state the following:

INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property further described in Attachment A—certain electronic devices, collectively the "Devices"—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent of the United States Immigration and Customs Enforcement, Homeland Security Investigations (HSI), presently assigned to the Human Trafficking Unit located at the Custom House, Baltimore, Maryland. I have been employed with HSI since March 2009. Your affiant is currently assigned to the Human Smuggling and Trafficking unit. As part of my daily duties as an HSI agent, I investigate criminal violations relating to human trafficking including sex and labor trafficking in violation of 18 U.S.C. §§ 1589, 1590 and 1591 as well as interstate transportation for prostitution (Mann Act) in violation of 18 U.S.C. § 2421. I have received training in the area of human trafficking and have also participated in the execution of search warrants which involved sex trafficking and sex trafficking of minors. I have received formal training from HSI and other agencies in the area of internet crimes and investigation

including the use of social networking sites and other internet facilities to coerce and/or facilitate prostitution of minors and adults in violation of 18 U.S.C. § 1591 and interstate prostitution (Mann Act) 18 U.S.C. § 2421.

3. As a federal agent, your Affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to affect arrests and execute warrants issued under the authority of the United States.

4. I respectfully submit that probable cause exists to believe that the electronic devices described in Attachment A contain evidence, and are themselves instrumentalities, of criminal conduct committed by Michael BOSWELL.

5. BOSWELL was charged in a criminal complaint on October 22, 2013, with violations of 18 U.S.C. §§ 371, 2421, 2422. SAG-13-2501. That same day, United States Magistrate Judge Stephanie A. Gallagher authorized a search warrant for email accounts connected with this investigation. SAG-13-2502 & 2503. In an Indictment returned by the Grand Jury for the District of Maryland on October 31, 2013, BOSWELL was charged with violations of 18 U.S.C. §§ 2421 & 2422.

DEVICES TO BE EXAMINED

6. The target electronic devices to be examined are described herein and further described in Attachment A. The Devices are currently in the lawful possession of HSI. The devices were recovered by state law enforcement officers on or about June 20, 2013, during the execution of search warrants by the Anne Arundel County Police Department. The location where each of the Devices was originally found is specified in Paragraph 17 below.

a. One Verizon Samsung cell phone, MEID A000004064A420.

b. One Virgin Mobile Kyocera cell phone, MEID A00000048F7552.

JSH

c. One Virgin Mobile LG cell phone, MEID A1000019434743.

d. One Cricket ZTE cell phone, MEID A00000322F0A0F.

e. One Samsung Galaxy Note II, IMEI 990002091277820.

f. One Sprint HTC cell phone, MEID A1000017C616D9.

g. Samsung micro SD card.

h. 16GB SanDisk Cruzer Switch thumb drive.

i. 4GB SanDisk Cruzer Glide thumb drive.

j. SIM card, serial number TF64PSIMC4B.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

8. The Devices are currently in storage at 40 S. Gay Street, Baltimore, Maryland. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of HSI.

9. Some of these devices were previously searched pursuant to state search warrants and/or as part of a search incident to arrest. Although your affiant believes that these searches were properly authorized, out of an abundance of caution this federal search warrant is sought before further searches of these electronic devices is conducted by federal investigators. None of the information gained from prior searches of these devices is used in this affidavit to establish probable cause for this search warrant.

10. Your affiant is familiar with the information contained in this Affidavit based upon the investigation your Affiant has conducted, and includes information from reports, witnesses, and other law enforcement officers. This affidavit is offered for the sole purpose of establishing

JSH

probable cause and does not include each and every fact known to law enforcement related to this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that evidence of violations of 18 U.S.C. §§ 2421, 2422 and 371, are contained on the target Devices.

PROBABLE CAUSE

11. On June 19, 2013, Anne Arundel County Police Department's (AAPD) Vice Unit initiated an investigation into suspected prostitution activity at the Microtel Hotel (Microtel) located at 1170 Winterson Road, Linthicum, MD 21090. On this date, AAPD detectives accessed the "Escort" section of the website Backpage.com and located an advertisement that depicted photos of a black-female in partially nude and provocative poses.[1] The advertisement displayed the phone number ***-***-2668 and instructed the potential customer to call or text this number to set up a "date." Investigators, based on their training experience, determined the advertisement was consistent with an offer for commercial sexual services.

12. Later on June 19, 2013, an AAPD detective, acting in an undercover capacity, sent a text to this same number stating that he just got off work, was looking for an hour long appointment, and wanted to know how much an hour appointment would cost. The detective received a text message in reply, asking if the undercover detective wanted to visit her at her location or meet at his location. The undercover detective replied that he wanted to meet at her location. The response to this stated that it would be $150 for an hour long appointment. The undercover detective also inquired about "backyard play," or anal sex, which increased the rate to $200. Upon agreeing to this amount, the undercover detective was then directed to the Microtel and

[1] Backpage.com is an online classified site that is commonly used to advertise for prostitution and sexual services.

more specifically, room 240. The undercover detective later canceled the "date;" but AAPD detectives maintained surveillance at the Microtel.

13. During that surveillance, AAPD detectives observed a black male, later identified as Michael Darnell BOSWELL (DOB **/**/1983), driving a white Ford Expedition with North Carolina registration "ZTE 3073." Detectives watched BOSWELL drive from the Microtel to a nearby Wendy's restaurant and 7-11. Upon his return to the Microtel, detectives observed BOSWELL enter room 240 with a Wendy's bag and then exit the room without it. Hotel records indicate that room 240 and also room 242 were registered to a female, later identified ("WITNESS1") with an arrival date of June 18, 2013 and a departure date of June 19, 2013 that was later extended to June 20, 2013, and both rooms were paid for in cash.

14. Detectives later surveilled BOSWELL driving the Ford Expedition to a nearby Walmart. Detectives observed WITNESS1 and a second female, later identified ("WITNESS2"), exit BOSWELL's vehicle and enter the Walmart. WITNESS1 and WITNESS2 later returned to the vehicle and were then driven by BOSWELL to the Microtel. Upon their return, AAPD detectives observed WITNESS1 and WITNESS2 enter room 240. BOSWELL remained in his vehicle at this time.

15. On June 20, 2013, AAPD detectives returned to the Microtel and observed the white Ford Expedition in the parking lot. At approximately 10:28 am, a different detective, acting in an undercover capacity, texted the phone number in the same Backpage ad from the previous day (***-***-2668). A text conversation was initiated and an outcall "date"[2] was set up between the undercover detective and the female in the Backpage ad at the Red Roof Inn located at 827 Elkridge Landing Road, Linthicum, MD.

[2] Based on my training and experience, I know that an "outcall" is an appointment for commercial sex where the prostitute travels to the customer's location.

JSH

16. After the "date" for commercial sex was set up, surveillance teams observed BOSWELL drive WITNESS1 in the Ford Expedition from the Microtel to the Red Roof Inn. The undercover detective directed WITNESS1 to room 236 at the Red Roof Inn. Once WITNESS1 entered the hotel room, the undercover detective asked her if she had a condom to which she replied "yes" and removed one from the small, black bag she was carrying. WITNESS1 was arrested by AAPD and charged with prostitution and related offenses. BOSWELL was also arrested at a nearby parking lot, and WITNESS2 was arrested at the Microtel in room 242. A search warrant was executed for rooms 240 and 242 at the Microtel and the Ford Expedition.

17. A number of items were recovered during these searches, including electronic devices (the "Devices") listed in Attachment A. BOSWELL was arrested after driving WITNESS1 in the Ford Expedition to a date with the undercover officer at the Red Roof Inn.

a. When BOSWELL was removed from the vehicle and placed under arrest, detectives found a **Samsung Galaxy Note 2 smartphone, IMEI 990002091277820** in the driver's seat. Other electronic devices recovered from the vehicle included a **Samsung micro SD card; a Virgin Mobile Kyocera cell phone, MEID A00000048F7552; a 16GB SanDisk Cruzer Switch thumb drive;** and a **4GB SanDisk Cruzer Glide thumb drive**. Other items seized from the vehicle included BOSWELL's court papers showing prior arrests for human trafficking, prostitution, etc.; western union receipts; receipts from hotels in Virginia; condoms; price list for sexual services; and a "pimp song."

b. I know from my training and experience that traffickers sometimes write "songs" about their lives, including pimping and prostitution. The songs often include slang associated with commercial sex acts, earning money, travel, "hoes," "pimpin," etc. At the time of the search warrant, AAPD detectives also recovered a handwritten "pimp song" in BOSWELL's

vehicle. The lyrics include phrases such as "...Pimpin hoes bank style money still my persona....I get coin to have a chick pop pussy for 4 + 0 5 dayz...I get it jumpin from NC to PA...Pimpings thes games you ant pimpin the same." This song describes BOSWELL's activities, including earning money from selling commercial sex acts from "hoes," and traveling from "NC" (North Carolina) to "PA" (Pennsylvania) to do so. This song is attached as Exhibit A.

c. During the search of Microtel room 240 a **Cricket ZTE cell phone, MEID A00000322F0A0F**, was seized. Other items that were recovered included a receipt for the Microtel with WITNESS1's name on it, receipts from hotels in Virginia, and a MoneyGram receipt.

d. During the search of Microtel room 242 a **Verizon Samsung cell phone, MEID A000004064A420; a Sprint HTC cell phone, MEID A1000017C616D9; and a SIM card with serial number TF64PSIMC4B** were recovered. When WITNESS1 was arrested in room 242 (as described above in paragraph 16), a **Virgin Mobile LG cell phone, MEID A1000019434743**, was found on her person during a search incident to arrest. Other items recovered included condoms; receipts from restaurants in Virginia; a piece of paper with "FBM 4 Lyfe" written on it; and Western Union receipts.

e. I believe that the context in which these devices were found shows that they were likely used in furtherance of violations of federal law, and will contain evidence of those violations. This includes communications between BOSWELL and prostitutes, communications with individuals paying for commercial sex acts, and communications and records of payments for Backpage advertisements and other means of facilitating prostitution.

18. In a voluntary interview, WITNESS1 provided information to law enforcement. She stated that BOSWELL recruited her at a party in North Carolina, and arranged for her to travel from Greensboro, NC, to Richmond, VA, via a Greyhound Bus that was purchased for her. This was corroborated by a Greyhound Bus ticket, in WITNESS1's name, for such a trip recovered during the search of the Microtel. Once in Richmond, WITNESS1 met up with BOSWELL and WITNESS2, and, at BOSWELL's direction, began working as a prostitute in Virginia. She also stated that BOSWELL transported her and WITNESS2 to Maryland for the purpose of further engaging in prostitution. She stated that BOSWELL would communicate directly with the sex customers, and then inform her when she had a "date" set up.

19. Pursuant to a subpoena to Backpage.com discussed above, Backpage provided records that showed, inter alia, that the customer account associated with the Backpage advertisement above had as its associated email address fbm.entertainment1@gmail.com. FBM Entertainment is a business owned by BOSWELL, as described below, Paragraph 21. Backpage requires account holders to provide an email address, which Backpage uses for all customer communications, such as confirmation of the posting of an advertisement, receipts for payments, and general account information. The subpoena response shows multiple advertisements for "escort services" consistent with advertisements for commercial sex (i.e. prostitution) were posted on Backpage.com with this same account from at least April 2013 through July 2013. These advertisements advertised services in various states including North Carolina, Virginia, Washington, DC and Maryland.

a. The subpoena response showed that the target Backpage account was used to post advertisements for commercial sexual services in Richmond, Northern Virginia and Maryland. For instance, on June 12, 2013, an advertisement for sexual services in Richmond, Virginia from

"Ms. Monroe" was posted, showing pictures of WITNESS2. A similar advertisement for sexual services in Richmond, Virginia from "Kimberly" (WITNESS1) was also posted. Similar advertisements were posted against on June 13, 2013.

b. On June 14, 2013, an advertisement for sexual services in Springfield/Northern Virginia from R.T was posted. A similar advertisement for WITNESS2 was reposed on the June 15, 16, and 17. A similar advertisement for sexual services in Springfield/Northern Virginia from WITNESS1 was also posted on June 16 and 17.

c. On June 18, 2013, Backpage ads were posted advertising sexual services by WITNESS2 and WITNESS1 in the Baltimore/BWI area. The IP addresses used to make these posts was registered to the Microtel where BOSWELL, WITNESS1 and WITNESS2 were staying at the time AAPD was conducting the undercover operation.

20. The Backpage subpoena also showed that most of the associated advertisements for commercial sex acts were paid for with American Express credit card ending with 9231. A subpoena to American Express showed that the American Express customer is Michael BOSWELL, DOB **/**/1983, 1500 Burgundy Street, Apt. A, Raleigh, NC 27610, phone number ***-***-9148. The American Express transaction records also show numerous payments made to BACKPAGE.COM and merchants in North Carolina, Virginia, and Maryland.

21. BOSWELL is a self-proclaimed "party planner" and owns a business called F.B.M. Party Planners (FBM) and Mobile Mixtape Entertainment. At the time of arrest, BOSWELL had in his wallet two business licenses for FBM and Mobile Mixtape. He also had an IRS Form 8832, Entity Classification Election, in his wallet, which contained the business name of Mobile Mixtape and an Employer Identification Number (EIN). These documents show both businesses are registered to the address 2010 Hodge Creek Drive, Apt. 104, Raleigh, NC 27609.

a. The website for FBM is fbm1entertainment.escort-site.com. An open-source review of this website confirmed that this website advertises escort services and prostitution. Under the "photos" section of the website there are multiple females, such as "Candy" and "Mz Slim," in partially nude photographs. The "services" section of the website indicates the types of services provided by FBM, such as "Fetish/Fantasy, Role Play, Mistress Worship." There is also a list on the site entitled "My Escort Services," which lists common terms used in prostitution and their definitions, such as "69 (69 sex), BJ (blow job), CBJ (Covered Blow Job; Oral sex with a condom)." The website also provides an email contact for customers wishing to obtain these sexual services.

b. The search warrant executed by AAPD at the Microtel also recovered a notepad with the term "FBM 4 Lyfe" handwritten on it. Furthermore, in a voluntary interview with your affiant, WITNESS2 stated that when she met BOSWELL at a party in North Carolina he gave her a business card with "FBM" on the front of it. BOSWELL told her that "FBM" stands for Future Black Millionaire.

c. In my training and experience, an individual operating a website advertising commercial sex acts needs to use internet-capable devices to communicate with prospective customers, as well as update and maintain the website.

22. BOSWELL was charged in in Anne Arundel County Circuit Court with various offenses, including Human Trafficking, Prostitution, and Possession of Marijuana. Those charges were dismissed, and he is presently detained pending trial on these federal charges.

23. Prior to his arrest in Maryland, BOSWELL had multiple arrests in New Jersey, North Carolina, and Virginia, including charges for prostitution and related offenses, as follows:

JSH

a. On November 24, 2010, BOSWELL was arrested and charged in Raleigh, North Carolina with 1) Possession of a Firearm by a Felon, 2) Possession of Marijuana Up to ½ Ounce, and 3) Aid and Abet Prostitution. On May 20, 2013, he was convicted of Possession of a Firearm by a Felon, which is a felony charged.

b. On April 20, 2011, BOSWELL was arrested and charged in Raleigh, North Carolina for Maintain Place for Prostitution, which was dismissed.

c. On May 3, 2012, BOSWELL was arrested in Henrico County, Virginia for 1) Two Counts of Prostitution: Receive Earnings (Pandering), 2) Possess Marijuana, 3) Prostitution: Aid, and 4) Prostitution: Keep/Reside in Bawdy Place. All charges were dismissed.

d. On January 4, 2013, BOSWELL was arrested in Henrico County, Virginia for 1) Prostitution: Use Vehicle to Aid, 2) Two Counts Prostitution: Aid, 3) Prostitution: Keep/Reside in Bawdy Place, 4) Weapon: Possess by Felon (Not Firearm), and 5) Possess Marijuana 2+ Offense. BOSWELL was found not guilty of Possess Marijuana 2+ Offense. There was no disposition for Weapon: Possess by Felon (Not Firearm) and all other charges were dismissed.

e. On March 11, 2013, BOSWELL was arrested and charged in Henrico County, Virginia for 1) Six counts of Prostitution: Receive Earnings (Pandering), 2) Prostitution: Aid, 3) Two counts of Prostitution: Use Vehicle to Aid, 4) Two counts of Prostitution: Cause Person to Enter Bawdy Place, and 5) Prostitution: Keep/Reside In Bawdy Place. BOSWELL was released on bond for these charges and was awaiting trial at the time he was arrested in Maryland. At the time of his arrest in Maryland, he was also on probation at the time for a prior firearm offense.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. There is probable cause to believe that things that were once stored on the electronic devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files.

Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data, with internal storage on a number of electronic devices containing slightly less. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

f. Thus, the ability to retrieve residue of an electronic file from a hard drive or internal storage of other types of electronic devices depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above described information will be recovered during forensic analysis.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

CONCLUSION

27. Based on your affiant's training and experience, your Affiant respectfully submits that probable cause exists to search the Devices listed in Attachment A. Therefore, I respectfully request that the attached warrant be issued authorizing the search of the Devices listed in Attachment A and the seizure of the items listed in Attachment B.

14-0557TJS 14-0558TJS

13-2995SAG JSH

I declare under penalty of perjury that the foregoing is true and correct.

Kate N. Reilly
Special Agent, Homeland Security Investigations

Sworn and subscribed to before me on this 18th day of December, 2013.

Hon. Stephanie A. Gallagher
United States Magistrate Judge

ATTACHMENT A

a. One Verizon Samsung cell phone, MEID A000004064A420;

b. One Virgin Mobile Kyocera cell phone, MEID A00000048F7552;

c. One Virgin Mobile LG cell phone, MEID A1000019434743;

d. One Cricket ZTE cell phone, MEID A00000322F0A0F;

e. One Samsung Galaxy Note II, IMEI 990002091277820;

f. One Sprint HTC cell phone, MEID A1000017C616D9;

g. Samsung micro SD card;

h. 16GB SanDisk Cruzer Switch thumb drive;

i. 4GB SanDisk Cruzer Glide thumb drive; and

j. SIM card with serial number TF64PSIMC4B.

ATTACHMENT B

1. All information and records on the devices described in Attachment A that relate to violations of 18 U.S.C. §§ 2421, 2422 and 371 and involve BOSWELL and possible co-conspirators, including:

a. the communications and records of communications between BOSWELL, WITNESS1, WITNESS2, and possible co-conspirators;

b. any information regarding prostitution and/or escort services, including information about individuals involved in prostitution and/or escort services, and any information regarding recruitment, enticement or travel for the purpose of prostitution and/or escort services;

c. any information regarding the advertising of prostitution and/or escort services, including all records and communications relating to Backpage.com, fbm1entertainment.escort-site.com, F.B.M. Party Planners (FBM), Mobile Mixtape Entertainment, and any other business or websites used to advertise prostitution and/or escort services;

d. any information showing association between BOSWELL, WITNESS1, WITNESS2, and any others involved in prostitution and/or escort services;

e. all bank records, checks, credit card bills, account information, and other financial records;

f. any and all evidence of passwords needed to access any of the subject devices;

g. any and all records, showing dominion, ownership, custody, or control over the any of the subject devices;

h. All records and communications related to travel and location, including reservations or payments for hotel rooms and transportation such as payments for gas, rental cars, Greyhound bus, Amtrak, airlines, or other modes of transportation.

2. Evidence of user attribution showing who used or owned the phones at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the Internet, including:

a. records of Internet Protocol addresses used;

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Any of the items described in paragraphs 1 through 3 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form. The search procedure of the electronic data contained in computer operating software or memory devices shall include the following techniques which shall be used to minimize the risk that those conducting the search will view information not within the scope of the warrant:

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

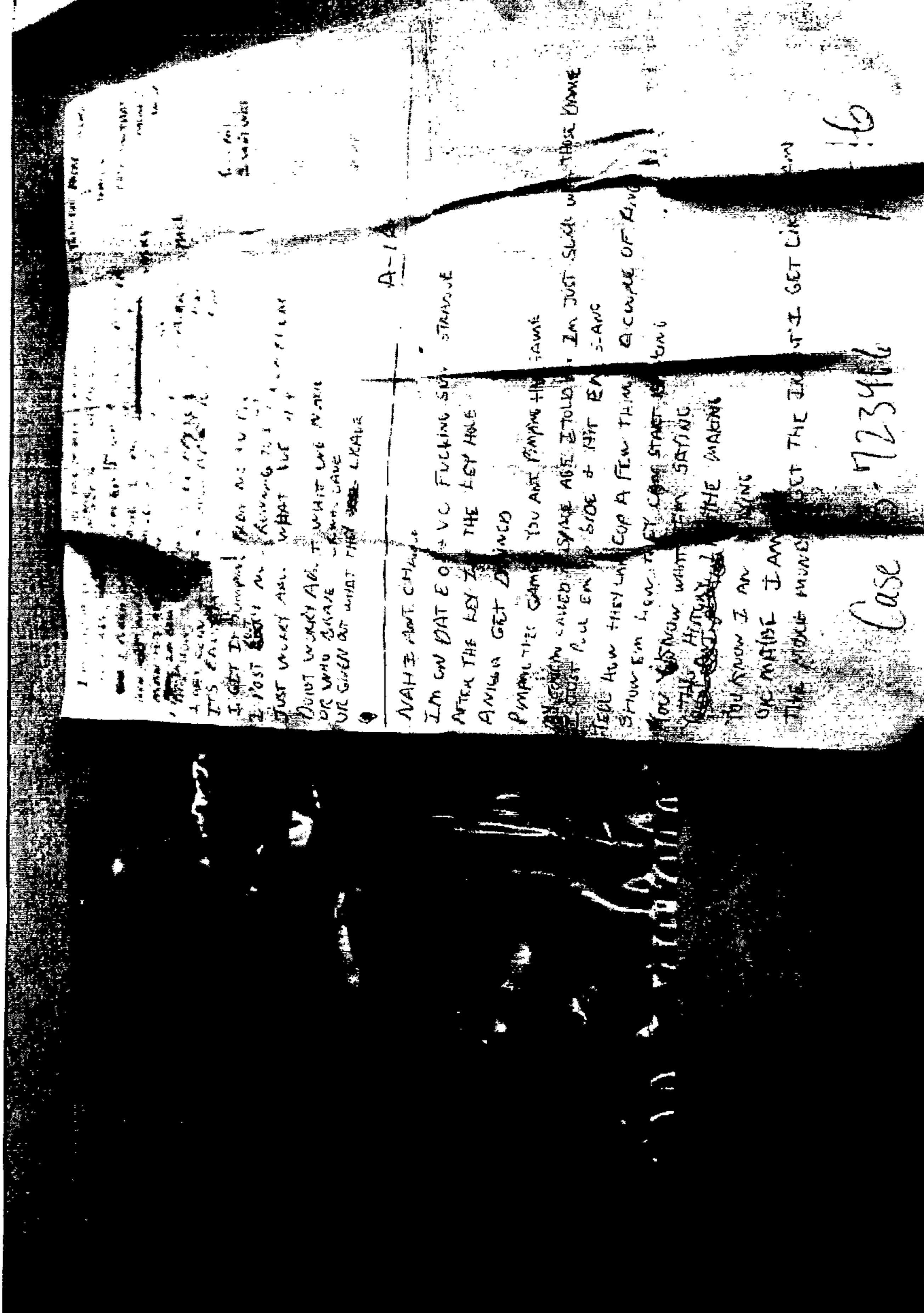
d. "scanning" storage areas for deliberately hidden files; or

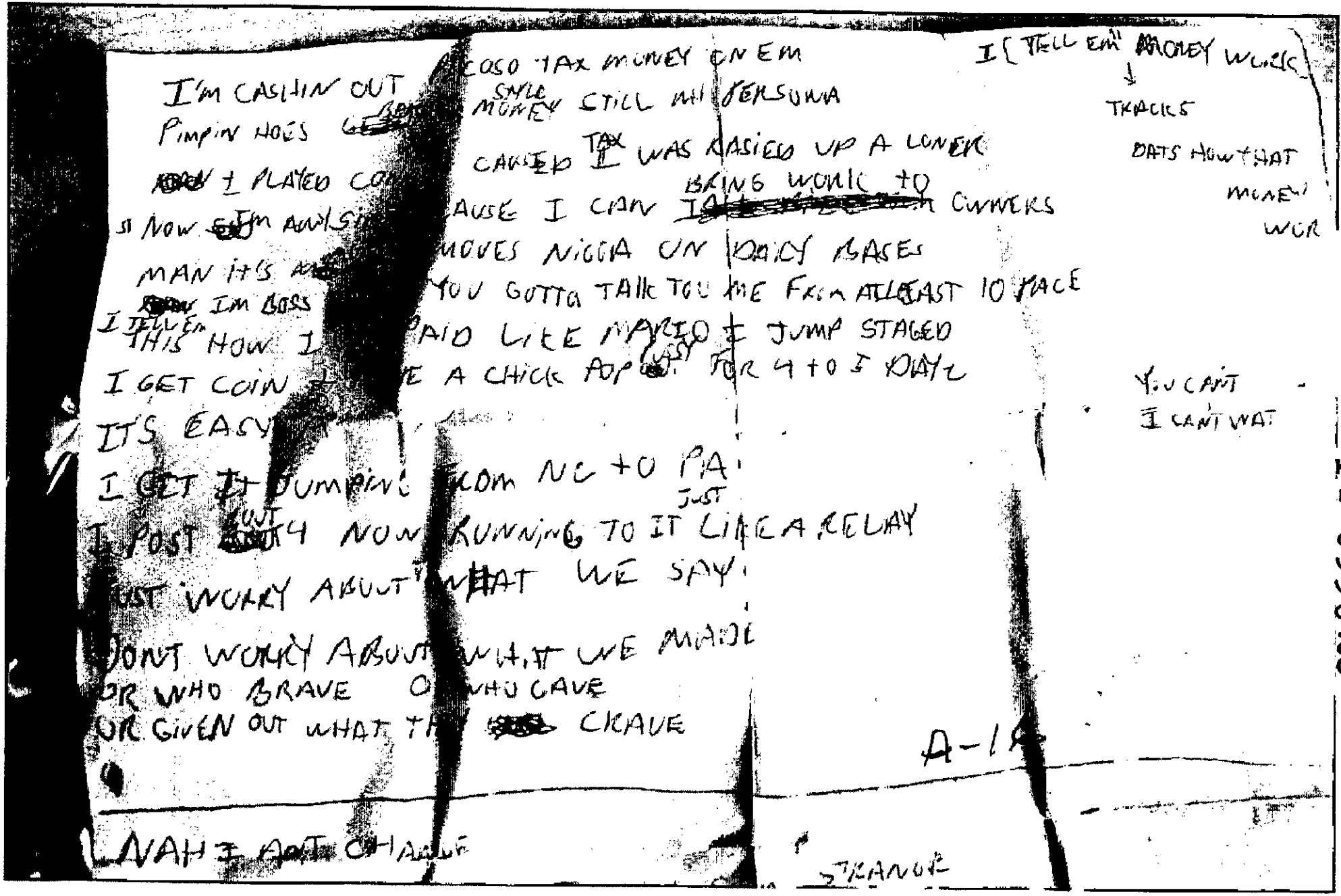
e. performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

4. If after performing these procedures, the directories, files or storage areas do not reveal evidence of violations of 18 U.S.C. §§ 2421, 2422 and 371, the further search of that particular directory, file or storage area, shall cease.

14-0557TJS 14-0558TJS

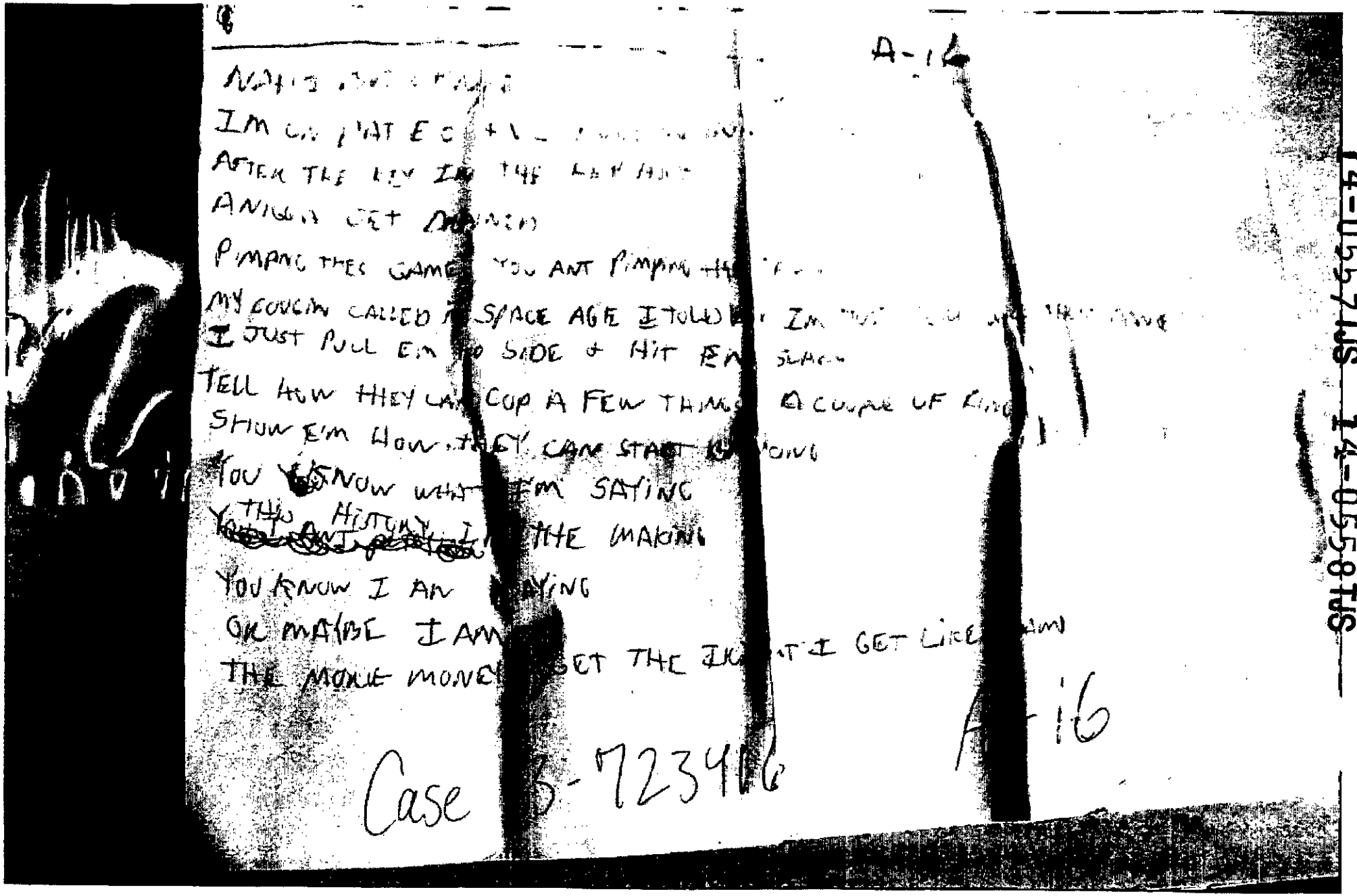
Exhibit A





I'M CASHIN OUT
PIMPIN HOES
I PLAYED CO
NOW IM ANGLIN
MAN IT'S A
IM BOSS
I TELL'EM THIS HOW I
I GET COIN
IT'S EASY
I GET IT DUMPIN
I POST UP
JUST WORRY ABOUT
DONT WORRY ABOUT
OR WHO BRAVE
OR GIVEN OUT WHAT
NAH I AIN'T
CASO TAX MONEY ON EM
STYLE
MONEY STILL MULTIPLYING
CARRIED TAX I WAS RAISED UP A LONER
BRING WORK TO
CAUSE I CAN
MOVES NIGGA ON
YOU GOTTA TALK TO ME FROM ATLEAST 10 PACE
PAID LIKE MARIO I JUMP STAGED
A CHICK
FOR 4 TO 5 DAYS
FROM NC TO PA
JUST
RUNNING TO IT LIKE A RELAY
WHAT WE SAY
WHAT WE MADE
WHO CAVE
CRAVE
I TELL EM MONEY WORK
TRACKS
DATS HOW THAT MONEY WOR
YOU CAN'T
I CAN'T WAT
A-1
TRANCE

14-0557TJS 14-0558TJS



A-14

I'M ON THAT E[illegible]

AFTER THE LIV IN THE [illegible]

ANIGGA GET [illegible]

PIMPING THEC GAME YOU AIN'T PIMPING [illegible]

MY COUSIN CALLED ME SPACE AGE I TOLD HIM I'M [illegible]

I JUST PULL EM TO SIDE & HIT EM [illegible]

TELL HOW THEY CAN COP A FEW THING A COUPLE OF [illegible]

SHOW EM HOW THEY CAN START [illegible]

YOU KNOW WHAT I'M SAYING

YOU KNOW THIS HISTORY IN THE MAKING

YOU KNOW I AM [illegible]

OK MAYBE I AM

THE MORE MONEY GET THE IKE I GET LIKE [illegible]

Case 3-723416

A-16

14-0557TUS 14-0558TUS